

日本国特許庁  
JAPAN PATENT OFFICE

23.04.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月17日  
Date of Application:

出願番号 特願2003-072371  
Application Number:

[ST. 10/C]: [JP 2003-072371]

出願人 セイコーエプソン株式会社  
Applicant(s):

REC'D 24 JUN 2004

WIPO

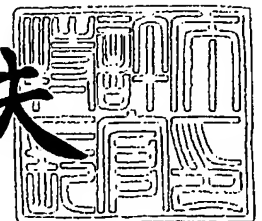
PCT

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 6月 2日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 J0096563

【あて先】 特許庁長官殿

【国際特許分類】 G06F 11/30

【発明者】

    【住所又は居所】 長野県諏訪市大和 3 丁目 3 番 5 号 セイコーエプソン株式会社内

    【氏名】 黒田 直人

【特許出願人】

    【識別番号】 000002369

    【氏名又は名称】 セイコーエプソン株式会社

【代理人】

    【識別番号】 100095728

    【弁理士】

    【氏名又は名称】 上柳 雅誉

    【連絡先】 0 2 6 6 - 5 2 - 3 1 3 9

【選任した代理人】

    【識別番号】 100107076

    【弁理士】

    【氏名又は名称】 藤網 英吉

【選任した代理人】

    【識別番号】 100107261

    【弁理士】

    【氏名又は名称】 須澤 修

【手数料の表示】

    【予納台帳番号】 013044

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0109826

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ウィルス対策システムとウィルス対策プログラムとウィルス対策方法とウィルス対策用端末装置

【特許請求の範囲】

【請求項 1】 周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設けた記憶手段と、

そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する手段と、

当該コンピュータの管理者宛の検出報告を発する手段と、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える手段を備えたことを特徴とするウィルス対策システム。

【請求項 2】 周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶させた記憶手段と、

そのおとりアプリケーションにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する手段と、

当該コンピュータの管理者宛の検出報告を発する手段と、

当該ウィルスの駆除が完了するまで、当該コンピュータに高負荷を与える手段を備えたことを特徴とするウィルス対策システム。

【請求項 3】 請求項 1 に記載のウィルス対策システムにおいて、

おとりフォルダは、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションから成ることを特徴とするウィルス対策システム。

【請求項 4】 請求項 2 に記載のウィルス対策システムにおいて、

おとりアプリケーションは、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションから成ることを特徴とするウィルス対策システム。

【請求項 5】 請求項 1 に記載のウィルス対策システムにおいて、

探索の対象となるウィルスは、共有フォルダへ侵入する性質を持つウィルスであることを特徴とするウィルス対策システム。

【請求項 6】 請求項 2 に記載のウイルス対策システムにおいて、  
探索の対象となるウイルスは、アプリケーションの誤動作を引き起こす性質を持つウイルスであることを特徴とするウイルス対策システム。

【請求項 7】 請求項 1 または 2 に記載のウイルス対策システムにおいて、  
感染したコンピュータに対して、高負荷を与える攻撃開始を予告するための、メッセージを送信する手段を備えたことを特徴とするウイルス対策システム。

【請求項 8】 請求項 1 に記載のウイルス対策システムにおいて、  
攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段を設けたことを特徴とするウイルス対策システム。

【請求項 9】 請求項 1 に記載のウイルス対策システムにおいて、  
コンピュータに高負荷を与える手段は、当該コンピュータのネットワークインタフェースのトラフィックを増大させる機能を持つことを特徴とするウイルス対策システム。

【請求項 1 0】 請求項 1 に記載のウイルス対策システムにおいて、  
コンピュータに高負荷を与える手段は、当該コンピュータの CPU が応答動作をすべき処理を大量に要求することを特徴とするウイルス対策システム。

【請求項 1 1】 請求項 1 に記載のウイルス対策システムにおいて、  
ネットワークに接続された別のコンピュータに対して、ウイルスの送信元となったコンピュータのネットワークアドレスを通知するとともに、ウイルスの送信元となったコンピュータに負荷を与える処理を依頼する手段を備えたことを特徴とするウイルス対策システム。

【請求項 1 2】 ウイルスの送信元となったコンピュータネットワークアドレスの通知を受けたとき、ウイルスの送信元となったコンピュータに負荷を与える処理を、コンピュータに実行させるウイルス対策プログラム。

【請求項 1 3】 ウイルスの送信元となったコンピュータネットワークアドレスの通知を受けたとき、ウイルスの送信元となったコンピュータからの通信を拒絶する処理を、コンピュータに実行させるウイルス対策プログラム。

【請求項 1 4】 周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設け、

そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出し、

当該コンピュータの管理者宛の検出報告を発するとともに、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えることを特徴とするウィルス対策方法。

【請求項 15】 周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶装置に記憶させ、

そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出し、

当該コンピュータの管理者宛の検出報告を発するとともに、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えることを特徴とするウィルス対策方法。

【請求項 16】 周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを記憶させた記憶装置と、

そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出するコンピュータプログラムと、

当該コンピュータの管理者宛の検出報告を発するコンピュータプログラムと、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えるコンピュータプログラムをインストールしたことを特徴とするウィルス対策用端末装置。

【請求項 17】 周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶させた記憶装置と、

そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出するコンピュータプログラムと、

、

当該コンピュータの管理者宛の検出報告を発するコンピュータプログラムと、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えるコンピュータプログラムとをインストールしたことを特徴とするウィルス対策用端末装置。

【請求項 18】 周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを記憶装置に記憶させる処理と、

そのフォルダにウイルスが侵入したときに取得した通信情報から、ウイルスの送信元となったコンピュータを検出する処理と、

当該コンピュータの管理者宛の検出報告を発する処理と、

当該ウイルスへの対策が完了するまで、当該コンピュータに高負荷を与える処理とを、コンピュータに実行させることを特徴とするウイルス対策プログラム。

【請求項 19】 周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶装置に記憶させる処理と、

そのアプリケーションにウイルスがアクセスしたときに取得した通信情報から、ウイルスの送信元となったコンピュータを検出する処理と、

当該コンピュータの管理者宛の検出報告を発する処理と、

当該ウイルスへの対策が完了するまで、当該コンピュータに高負荷を与える処理とを、コンピュータに実行させることを特徴とするウイルス対策プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークに接続されたコンピュータがウイルスに感染したとき、感染源を突き止めて、同じネットワークに接続された他のコンピュータへの感染を阻止する機能を持つ、ウイルス対策システムとウイルス対策プログラムとウイルス対策方法とウイルス対策用端末装置に関する。

【0002】

【従来の技術】

コンピュータウイルスには、サーバ等のコンピュータの共有フォルダに侵入して、所定のファイルやプログラムにアクセスをし、それを破壊したり、誤動作させるように書き換えたりするものがある。ウイルスの存在は、所定のプログラムを使って検出することができる。このプログラムは、ウイルスのファイル名やウイルスの行動パターンから、ウイルスであると判断をする。ウイルスを検出すると、コンピュータの管理者は必要な処置を施し、ウイルスを除去する。こうしてウ

ウイルスを検出してワクチンを配布する技術は、各種紹介されている（特許文献1参照）。

【特許文献1】 特開2002-259149号公報

【0003】

【発明が解決しようとする課題】

ところで、上記のような従来の技術には、次のような解決すべき課題があった。

ウィルスを検出したときは、すみやかにその存在場所を突き止めて、ネットワークから切り離したり、ワクチンを用いて駆除するという処理をしなければならない。しかしながら、ウィルスを検出してから対策処理を完了するまでの間に時間がかかると、次々と被害が拡大して、ネットワークに重大な被害を及ぼす恐れもある。

また、ネットワーク上の別のコンピュータに潜んで、ネットワークを通じてファイルアクセスをしてくるようなウィルスは、活動を開始するまで検出が困難なことがある。そのウィルスが活動を開始し、ウィルスを検出したとしても、ウィルスの潜んでいるコンピュータを調べて、そのウィルスを駆除するまで時間がかかると、被害が拡大するという問題があった。

【0004】

本発明は、以上の点に着目してなされたもので、ネットワークに接続されたコンピュータがウィルスに感染していることを突き止めると同時に、同じネットワークに接続された他のコンピュータへの被害の拡大を阻止するように、ウィルスに感染したコンピュータを攻撃する、ウィルス対策システムとウィルス対策プログラムとウィルス対策方法とウィルス対策用端末装置を提供することを目的とする。

さらに本発明は、活動を開始するまで検出活動ができないようなウィルスをいち早く検出して、被害の拡大を抑えることができるウィルス対策システムとウィルス対策プログラムとウィルス対策方法とウィルス対策用端末装置を提供することを目的とする。

【0005】



**【課題を解決するための手段】**

本発明は次の構成により上記の課題を解決する。

**〈構成 1〉**

周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設けた記憶手段と、そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する手段と、当該コンピュータの管理者宛の検出報告を発する手段と、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える手段を備えたことを特徴とするウィルス対策システム。

**【0006】**

ネットワーク監視用のコンピュータに、周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設けることで、最先にウィルスの侵入を促す。ウィルスが侵入をしたとき、直ちに感染源を突き止めて、被害の拡大を防止した上で対策を施す。ウィルスの侵入とは、ウィルスが、ネットワークを通じて、フォルダ中の任意のファイルを読み出したり、ファイルの書き換えを試みたりすることである。ウィルスに感染するというのは、ウィルス自体がコンピュータの記憶装置のどこかに取り込まれていることをいう。通信情報は、ウィルスがおとりフォルダに侵入をしたときにネットワークから受信した通信経路等の情報である。この通信情報中に、ウィルスの送信元となったコンピュータのネットワークアドレス等が含まれる。ウィルスの送信元となったコンピュータは、ウィルスに感染したコンピュータである。おとりフォルダで待ち受けるので、侵入してきたウィルスを検出できる。検出報告の内容は任意である。報告方法も任意である。感染したコンピュータの管理者に通知すると同時にその感染源のコンピュータを攻撃する。ウィルスの駆除が完了するまで、攻撃を継続する。攻撃するには、コンピュータに高負荷を与える。ウィルス対策とは、感染コンピュータをネットワークから切り離したり、あるいは、ウィルスを駆除することである。

**【0007】****〈構成 2〉**

周辺に設けられているアプリケーションと比較して、セキュリティの低いおと

りのアプリケーションを記憶させた記憶手段と、そのおとりアプリケーションにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する手段と、当該コンピュータの管理者宛の検出報告を発する手段と、当該ウィルスの駆除が完了するまで、当該コンピュータに高負荷を与える手段を備えたことを特徴とするウィルス対策システム。

#### 【0008】

構成1はおとりフォルダを設けたものであるが、構成2では、おとりアプリケーションを設ける。おとりアプリケーションにウィルスが侵入したというのは、おとりアプリケーションをアクセスしたり、おとりアプリケーションに対するコマンドを送り込んだり、おとりアプリケーションの書き換えを試みたりすることである。

#### 【0009】

##### 〈構成3〉

構成1に記載のウィルス対策システムにおいて、おとりフォルダは、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションから成ることを特徴とするウィルス対策システム。

#### 【0010】

サーバへ侵入する性質を持つウィルスを検出する。おとりサーバは、擬似的なアプリケーションから成り、みかけ上サーバの構成を持つデータから成る。アクセスがあると、そのアクセスに対してサーバと同様の応答を返す機能を持つ。ウェブサーバでもメールサーバでも構わない。サーバ攻撃型のウィルスに対応するための構成である。コンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に、おとりフォルダを設けた構成にしたので、ウィルスの攻撃を受けてもその影響を受けない。すなわち、被害は発生しない。同時に、攻撃を受けながら、その出所を突き止めることができる。おとりサーバとおとりフォルダとは、全く別のものでも、一体化したアプリケーションから成るものでも構わない。

#### 【0011】

##### 〈構成4〉

構成2に記載のウィルス対策システムにおいて、おとりアプリケーションは、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションから成ることを特徴とするウィルス対策システム。

#### 【0012】

これも、サーバへ侵入する性質を持つウィルス検出のための構成で、おとりフォルダの代わりにおとりアプリケーションを設けた例である。

#### 【0013】

##### 〈構成5〉

構成1に記載のウィルス対策システムにおいて、探索の対象となるウィルスは、共有フォルダへ侵入する性質を持つウィルスであることを特徴とするウィルス対策システム。

#### 【0014】

共有フォルダへ侵入するウィルスは、おとりフォルダを設けることで、その活動を検出できる。

#### 【0015】

##### 〈構成6〉

構成2に記載のウィルス対策システムにおいて、探索の対象となるウィルスは、アプリケーションの誤動作を引き起こす性質を持つウィルスであることを特徴とするウィルス対策システム。

#### 【0016】

アプリケーションの誤動作を引き起こす性質を持つウィルスに対しては、擬似的なおとりアプリケーションを設けることで、その活動を検出できる。

#### 【0017】

##### 〈構成7〉

構成1または2に記載のウィルス対策システムにおいて、感染したコンピュータに対して、高負荷を与える攻撃開始を予告するための、メッセージを送信する手段を備えたことを特徴とするウィルス対策システム。

#### 【0018】

コンピュータのウィルス感染の報告をするとともに、その感染コンピュータに対して、攻撃開始を予告するメッセージを送信して、コンピュータの利用者や管理者に注意を促すことができる。

#### 【0019】

##### 〈構成8〉

構成1に記載のウィルス対策システムにおいて、攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段を設けたことを特徴とするウィルス対策システム。

#### 【0020】

攻撃元コンピュータから警報音を発生させることで、感染コンピュータとネットワークを共有している他の端末装置の利用者に注意を促すことができる。警報音の種類は任意である。また、ディスプレイに攻撃動作中の表示をしてもよい。

#### 【0021】

##### 〈構成9〉

構成1に記載のウィルス対策システムにおいて、コンピュータに高負荷を与える手段は、当該コンピュータのネットワークインタフェースのトラフィックを増大させる機能を持つことを特徴とするウィルス対策システム。

#### 【0022】

感染したコンピュータのネットワークインタフェースのトラフィックを増大させれば、そのネットワークインタフェースを通じた当該ウィルスによる感染の拡大が阻止できる。トラフィックを増大させる方法は任意である。

#### 【0023】

##### 〈構成10〉

構成1に記載のウィルス対策システムにおいて、コンピュータに高負荷を与える手段は、当該コンピュータのCPUが応答動作をすべき処理を大量に要求することを特徴とするウィルス対策システム。

#### 【0024】

例えば、Pingパケットを大量に連続的に送信する。これにより、CPUが過負荷になるので、コンピュータの内部でのウィルスの活動を阻止し、被害の拡

大を抑制できる。

#### 【0025】

##### 〈構成11〉

構成1に記載のウィルス対策システムにおいて、ネットワークに接続された別のコンピュータに対して、ウィルスの送信元となったコンピュータのネットワークアドレスを通知するとともに、ウィルスの送信元となったコンピュータに負荷を与える処理を依頼する手段を備えたことを特徴とするウィルス対策システム。

#### 【0026】

感染コンピュータへの攻撃が不十分である場合には、他のコンピュータに通知を行い、共同で攻撃をするように依頼する。依頼方法は任意である。他のコンピュータからの攻撃方法は任意である。それぞれ別々の方法でも構わない。

#### 【0027】

##### 〈構成12〉

ウィルスの送信元となったコンピュータネットワークアドレスの通知を受けたとき、ウィルスの送信元となったコンピュータに負荷を与える処理を、コンピュータに実行させるウィルス対策プログラム。

#### 【0028】

ネットワーク監視用のコンピュータから、感染コンピュータを攻撃する依頼を受けたときに、その処理を実行するプログラムの発明である。ネットワークに接続された任意のコンピュータにインストールされる。このコンピュータは、ネットワーク監視機能をもっているてもよいし、攻撃機能のみを持つものでもよい。

#### 【0029】

##### 〈構成13〉

ウィルスの送信元となったコンピュータネットワークアドレスの通知を受けたとき、ウィルスの送信元となったコンピュータからの通信を拒絶する処理を、コンピュータに実行させるウィルス対策プログラム。

#### 【0030】

ネットワーク監視用のコンピュータから、感染コンピュータの通知を受けたとき、防御のためにウィルスの送信元となったコンピュータからの通信を拒絶する

処理を実行するコンピュータプログラムの発明である。

【0031】

〈構成14〉

周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設け、そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出し、当該コンピュータの管理者宛の検出報告を発するとともに、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えることを特徴とするウィルス対策方法。

【0032】

構成1のシステムを運用する方法の発明である。

【0033】

〈構成15〉

周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶装置に記憶させ、そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出し、当該コンピュータの管理者宛の検出報告を発するとともに、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えることを特徴とするウィルス対策方法。

【0034】

構成2のシステムを運用する方法の発明である。

【0035】

〈構成16〉

周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを記憶させた記憶装置と、そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出するコンピュータプログラムと、当該コンピュータの管理者宛の検出報告を発するコンピュータプログラムと、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えるコンピュータプログラムをインストールしたことを特徴とするウィルス対策用端末装置。

## 【0036】

構成1のシステムでおとりフォルダを有する監視コンピュータの発明である。

## 【0037】

## 〈構成17〉

周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶させた記憶装置と、そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出するコンピュータプログラムと、当該コンピュータの管理者宛の検出報告を発するコンピュータプログラムと、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えるコンピュータプログラムとをインストールしたことを特徴とするウィルス対策用端末装置。

## 【0038】

構成2のシステムでおとりアプリケーションを有する監視コンピュータの発明である。

## 【0039】

## 〈構成18〉

周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを記憶装置に記憶させる処理と、そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する処理と、当該コンピュータの管理者宛の検出報告を発する処理と、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える処理とを、コンピュータに実行させることを特徴とするウィルス対策プログラム。

## 【0040】

構成1のシステムを実現するためのコンピュータプログラムの発明である。

## 【0041】

## 〈構成19〉

周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶装置に記憶させる処理と、そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となっ

たコンピュータを検出する処理と、当該コンピュータの管理者宛の検出報告を発する処理と、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える処理とを、コンピュータに実行させることを特徴とするウィルス対策プログラム。

#### 【0042】

構成2のシステムを実現するためのコンピュータプログラムの発明である。

#### 【0043】

##### 【発明の実施の形態】

以下、本発明の実施の形態を、具体例を用いて説明する。

図1は、ウィルス対策システム的具体例を示すブロック図である。

ネットワーク1には、ネットワークインタフェース4を介してコンピュータ5が接続されている。このコンピュータ5には、記憶装置6が設けられている。この記憶装置6に、ウィルス7が感染している。このコンピュータ5を感染コンピュータと呼ぶことにする。ネットワーク1には、監視コンピュータ10が接続されている。監視コンピュータ10は、ネットワークインタフェース11と記憶装置12とを備える。記憶装置12には、おとりサーバ13と、おとりフォルダ14と、おとりアプリケーション15とが記憶されている。さらに、ネットワークインタフェース11で取得される通信情報を監視するために、通信情報解析手段16が設けられている。通信情報解析手段16の出力は、警報発生手段19を駆動する。さらに、通信情報解析手段16の出力に基づいて、コンピュータ攻撃手段17と検出報告送信手段18とが動作するように構成されている。通信情報解析手段16とコンピュータ攻撃手段17と検出報告送信手段18と警報発生手段19はいずれも、監視コンピュータ10に所定の処理を実行させるコンピュータプログラムである。

#### 【0044】

この発明は、ウィルス7に感染しているコンピュータ5を特定し、そのコンピュータ5の管理者がウィルス7を除去するまでの間、そのコンピュータ5に高負荷を生じさせ、ウィルス7の活動を抑制する。ウィルス7に感染しているコンピュータ5を特定するために、おとりサーバ13やおとりフォルダ14やおとりア



アプリケーション 15 をネットワーク 1 中に構築する。おとりサーバ 13 等は、監視コンピュータ 10 中に擬似的に生成する。おとりフォルダ 14 は監視コンピュータ 10 の記憶装置 12 中の、任意の場所に生成するとよい。また、あるいは、おとりサーバ 13 中に一体に生成する。

#### 【0045】

##### [おとりサーバ等]

おとりのサーバ 13 は、ネットワーク 1 上で最先にウィルス 7 が攻撃してくるような環境設定をすることが好ましい。セキュリティを最も低くするとともに、例えば、コンピュータ名は、ネットワークコンピュータリストの最も上位に表示されるような名称に選定する。また、ウィルスを受け入れるための共有フォルダ名は、ウィルスがアタックしやすい性質のフォルダ名とする。これも、共有フォルダリストの最も上位に表示されるような名称に選定するとよい。また、コンピュータ名もフォルダ名も、ウィルスの性質から最適なものを決定するとよい。例えば、おとりサーバ 13 は、ウィルス 7 が実在のサーバに対して侵入を試みた場合の応答と全く同様の応答をするように動作するアプリケーションプログラムからなる。実在のサーバとは異なるから、破壊活動に対しては何の影響もない。例えばフォルダ 14 は、ウィルス 7 が実在のフォルダに対してアクセスした場合の応答と全く同様の応答をするように動作するアプリケーションプログラムからなる。実在のフォルダとは異なるからファイルの削除といった破壊活動に対して何の影響もない。おとりアプリケーション 15 は、実際のアプリケーションとは異なるから、誤動作を引き起こされる恐れはない。

#### 【0046】

##### [感染コンピュータの特定]

通信情報解析手段 16 には、ウィルスの侵入を検出すると、直ちにその通信情報中から発信源のコンピュータ名を解析して、特定する機能を持つ。この情報には、誰がログオンしたコンピュータか、そのコンピュータのアドレスは何か、コンピュータを使用している社員の社員コードは何か、といった情報が含まれる。なお、コンピュータウィルスを発見した場合に、無条件に直ちに感染しているコンピュータを攻撃すると、使用者がとまどって様々な弊害が生じる。そこで、警

報発生手段19を設ける。警報発生手段19は、例えば、ポップアップメッセージなどの通知手段を使って、感染コンピュータに対し、「このコンピュータはウィルスに感染しています。早急にネットワークから切り離してください」といった対策開始を予告するメッセージを送信する機能を持つ。さらに、周辺のコンピュータ利用者に対し、ネットワークを通じて、ウィルス7が侵入する恐れがある旨の警告を発するために、例えば、スピーカ2を鳴らしたりディスプレイ3に警報画面を表示したりする機能を持つ。

#### 【0047】

図2は、検出報告の例を示す説明図である。

通信情報解析手段16(図1)は、通信情報から取得した送信元IPアドレス8を検出報告送信手段18に転送する。検出報告送信手段18は、感染コンピュータ5の管理者に対して、例えば、電子メールやファクシミリを利用して、検出報告を送信する。(a)は拡散型のウィルスを検出したときの検出報告例である。(b)は、ネットワーク共有型のウィルスを検出したときの検出報告例である。例えば、(a)では、IPアドレスが「192.168.10.15」のコンピュータに、図のようなパタンのウィルスによる攻撃がされている。といった報告である。

#### 【0048】

##### [ウィルスの侵入と感染コンピュータの検出]

ウィルスが、ネットワーク上のいずれかのコンピュータに取り込まれると、所定のタイミングで活動を開始する。例えば、ウィルスは、ネットワークを通じて他のコンピュータの共有フォルダをアクセスして、そこに格納されたファイルを書き換えたり破壊したりする。ウィルスが侵入するというのは、このように、共有フォルダをアクセスする行為のことをいう。ウィルスファイルが実際にコピーされるとは限らない。従って、ウィルスが侵入されたコンピュータでは、通常の状態では、ウィルスの侵入によるファイルのアクセスか、正常なファイルのアクセスかを区別できず、ウィルスを検出できないこともある。

#### 【0049】

そこで、おとりサーバやおとりフォルダを設ける。通常のアプリケーションは、予め特定したサーバやフォルダにのみアクセスする。擬似的に作成された、お

とりサーバやおとりフォルダにアクセスするのは、ウィルスである確率が極めて高い。さらに、そのアクセスパターンを確認することで、ウィルスであるとの確証を得ることができる。その後は、その通信情報から、どのコンピュータがそのウィルスに感染したかを突き止める。感染コンピュータでのウィルスの活動を阻止しなければ、このウィルスがネットワークを通じて様々なコンピュータに被害を及ぼす。

#### 【0050】

コンピュータ攻撃手段17(図1)は、感染コンピュータに対して所定の攻撃動作をする機能を持つ。このコンピュータ攻撃手段17は、感染コンピュータ5に対して、高い負荷をかける。感染コンピュータ中のウィルスの活動を阻止するためであるから、感染コンピュータ5に対して高い通信負荷をかける方法と、感染コンピュータのCPUに高い負荷をかける方法がある。感染コンピュータ5に対して高い通信負荷をかけると、ネットワーク1と感染コンピュータとの間を結ぶネットワークインタフェース11等の通信路でトラフィックが増大して、感染コンピュータ5からネットワーク1に対する通信の通信速度が著しく低下する。従って、感染コンピュータ内部からネットワーク1を経由して他のコンピュータに向かうウィルスの侵入活動が抑制される。具体的には、100BASE-T程度の帯域を持つネットワークならば、5メガバイト程度もある大きなパケットを感染コンピュータ宛に送信するとよい。しかしながら、この場合、CPU自体にはさほどの負荷はかからない。一方、感染コンピュータのCPUに高い負荷をかけると、感染コンピュータの内部でデータの破壊活動をしようとするウィルスの活動速度が著しく低下する。従って、感染コンピュータ中にウィルス被害が広がるのを防止できる。具体的には、2バイト程度のPingパケットを感染コンピュータ5に向けて大量に連続的に送信する。感染コンピュータ5のCPUは、パケットを受信する度に応答を返すための制御をしなければならないので、CPUが過負荷になる。従って、上記の一方または両方の方法を併用するとよい。もちろん、上記以外の既知の任意の方法で、感染コンピュータに対して、高い負荷をかけるようにしてもよい。

#### 【0051】

## [他のコンピュータによる攻撃]

図3は、複数のコンピュータにより、感染コンピュータ5を攻撃する例を示す説明図である。

図のネットワーク1には、監視コンピュータ10に感染コンピュータ5のほか、端末装置20と端末装置22と端末装置24とが接続されている。端末装置20は、ネットワークインタフェース21を介してネットワーク1に接続されている。端末装置22は、ネットワークインタフェース23を介してネットワーク1に接続されている。端末装置24は、ネットワークインタフェース25を介してネットワーク1に接続されている。端末装置20と端末装置22と端末装置24とは、それぞれ、コンピュータ攻撃手段31とコンピュータ攻撃手段32とコンピュータ攻撃手段33とを備えている。コンピュータ攻撃手段31とコンピュータ攻撃手段32とコンピュータ攻撃手段33とはいずれも、監視コンピュータ10のコンピュータ攻撃手段17と同様の機能を持つ。

## 【0052】

1台のコンピュータで感染コンピュータを攻撃するのが不十分ならば、図のようにして、別のコンピュータに攻撃を依頼して、複数台のコンピュータの協力によって1台のコンピュータを攻撃する。これによって、ウィルスが感染したコンピュータの機能を制限し、その間に管理者に通知して、ウィルスを削除するための時間を稼ぐ。端末装置20等は、攻撃専用のコンピュータでもよいし、一般ユーザの使用しているコンピュータにコンピュータ攻撃手段31等をインストールしたものでもよい。監視コンピュータ10は、ネットワーク1中に1台だけ設けても、複数台設けても構わない。なお、監視コンピュータ10からコンピュータ攻撃手段31等に送信する攻撃依頼には、感染コンピュータのIPアドレス（ネットワークアドレス）を含める。また、コンピュータ攻撃手段31等を起動するコマンドを含めるとよい。コンピュータ攻撃手段を持つコンピュータは、監視コンピュータと同様の機能を持つコンピュータでもよいし、攻撃手段のみを持つコンピュータでもよい。

## 【0053】

図4は、大規模なコンピュータネットワークの説明図である。

図のように、ルータ 50 とルータ 51 とにより相互に接続されたネットワーク 52 とネットワーク 53 とネットワーク 54 には、それぞれ、多数のコンピュータが接続されている。ネットワーク 52 に接続されたコンピュータ 61 と 62 のうち、コンピュータ 62 は監視コンピュータである。ネットワーク 53 に接続されたコンピュータ 63 と 64 と 65 のうち、コンピュータ 63 は監視コンピュータである。ネットワーク 54 に接続されたコンピュータ 66 と 67 と 68 のうち、コンピュータ 68 は監視コンピュータである。例えば、コンピュータ 67 が感染コンピュータであって、コンピュータ 62 がそのウィルスの侵入を検知することがある。このときは、コンピュータ 62 から攻撃をしても、ルータ 50 やルータ 51 がネックになって、効果的な攻撃が難しい。そこで、コンピュータ 62 は、コンピュータ 67 の所属するネットワーク 54 に接続された最寄りのコンピュータ 68 に対して、コンピュータ 67 への攻撃を依頼する。コンピュータ 68 は先に説明したスピーカ等による警報を発して、周囲のコンピュータ 66 等に注意を促してから、コンピュータ 67 への攻撃を開始する。こうして、大規模なネットワークにおける監視動作も可能になる。

#### 【0054】

##### [動作フローチャート]

図 5 は監視コンピュータの基本動作を示すフローチャートである。

まず、ステップ S1 において、監視コンピュータ 10 は、おとりサーバ 13 やおとりフォルダ 14 やおとりアプリケーション 15 を有効にする初期設定をして、ステップ S2 で、ウィルスの待ち受けを開始する。通信情報解析手段 16 は、ネットワークインタフェース 11 の処理する通信情報を監視する。ステップ S3 で、ウィルスの侵入を検知すると、通信情報解析手段 16 は、ステップ S4 で通信情報の解析をして、ステップ S5 で送信元 IP アドレス 8 を取得し、感染コンピュータを特定する。検出報告送信手段 18 は、ステップ S6 で管理者へ検出報告をする。

#### 【0055】

警報発生手段 19 は、ステップ S7 で、スピーカ 2 による警報音を鳴らす。同時に攻撃中である旨の動画等を、監視コンピュータ 10 のディスプレイ 3 に表示

する。ステップS 8で、警報発生手段1 9は、感染コンピュータ5に対して攻撃開始メッセージを送信する。コンピュータ攻撃手段1 7は、ステップS 9で攻撃を開始する。その後のステップS 1 0で、任意のルートでウィルス対策が完了した旨を報告を受けたと判断すると、ステップS 1 1に進んで、コンピュータ攻撃手段1 7による攻撃を終了する。

#### 【0056】

図6は、監視コンピュータの協力動作を示すフローチャートである。

複数のコンピュータの協力を得て感染コンピュータを攻撃するときは、まず、感染コンピュータを特定する。ステップS 2 1～ステップS 2 4の処理は、ステップS 2～ステップS 5の処理と同様である。感染コンピュータを特定したら、ステップS 2 5で、コンピュータ攻撃手段1 7がネットワークの調査をする。最寄りの監視コンピュータを探すためである。最寄りの監視コンピュータを探すには、予め用意した監視コンピュータのリストから、感染コンピュータとIPアドレスの一部が共通している監視コンピュータを検索する（ステップS 2 6）。

#### 【0057】

最寄りの監視コンピュータが、自分自身である場合と、図4で説明したように、ルータのような幾つかのネットワークコンポーネントを介して接続された監視コンピュータである場合とがある。ステップS 2 7では、最寄りの監視コンピュータが自分自身かどうかを判断して、自分自身でなかったら、ステップS 2 8で攻撃依頼先を決定する。該当する監視コンピュータが複数ある場合は、複数の監視コンピュータに同報送信で攻撃依頼を発信すればよい。続いて、ステップS 2 9で、該当する監視コンピュータに対して、攻撃依頼の発信をする。その後は、攻撃依頼先において、図5のステップS 6以降の処理が実行される。

#### 【0058】

##### [感染コンピュータの処置]

感染コンピュータは被害を受けている可能性が高いので、すみやかにネットワークから切り離すことが最も効果的な対策である。この対策が完了すれば、感染コンピュータへの攻撃は終了してよい。感染コンピュータは、その後、ウィルスの除去処理をして、被害があった部分を修復したり、OS（オペレーティングシ

ステム) やアプリケーションの再インストールをして復旧させる。このために、図3に示すように、記憶装置6には、その旨のメッセージを含む画面40をディスプレイに表示する。この画面40は、必要な対応措置が終了後ボタン41がクリックされるまで表示される。

#### 【0059】

この発明は、ネットワークを通じて拡散するタイプのウィルスの拡散スピードを低下させる機能を持つ。すなわち、ウィルスが感染したコンピュータに大きな負荷をかけることによって、ウィルスの拡散を防止する。また、ウィルスが、あるコンピュータの共有ファイルに侵入しても、その動作だけでは侵入を直ちに確認することができない場合に適する。すなわち、ウィルスが活動したとき、そのウィルスの攻撃を真っ先に受けるようにおとりのコンピュータを設定する。これによって、ウィルスを発見し、ウィルスがどのコンピュータに感染しているかを確認し、該当する攻撃対象のコンピュータを特定する。すなわち、単にフォルダ内に侵入しただけでは、発見の難しいウィルスの検出と排除に有効である。

#### 【0060】

なお、上記のコンピュータプログラムは、それぞれ独立したプログラムモジュールを組み合わせて構成してもよいし、全体を一体化したプログラムにより構成してもよい。コンピュータプログラムにより制御される処理の全部または一部を同等の機能を備えるハードウェアで構成しても構わない。また、上記のコンピュータプログラムは、既存のアプリケーションプログラムに組み込んで使用してもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えばCD-ROMのようなコンピュータで読み取り可能な記録媒体に記録して、任意の情報処理装置にインストールして利用することができる。また、ネットワークを通じて任意のコンピュータのメモリ中にダウンロードして利用することもできる。

#### 【図面の簡単な説明】

【図1】 ウィルス対策システムの具体例を示すブロック図である。

【図2】 検出報告の例を示す説明図である。

【図3】 複数のコンピュータにより感染コンピュータを攻撃する例を示す説

明図である。

【図 4】 大規模なコンピュータネットワークの説明図である。

【図 5】 監視コンピュータの基本動作を示すフローチャートである。

【図 6】 監視コンピュータの協力動作を示すフローチャートである。

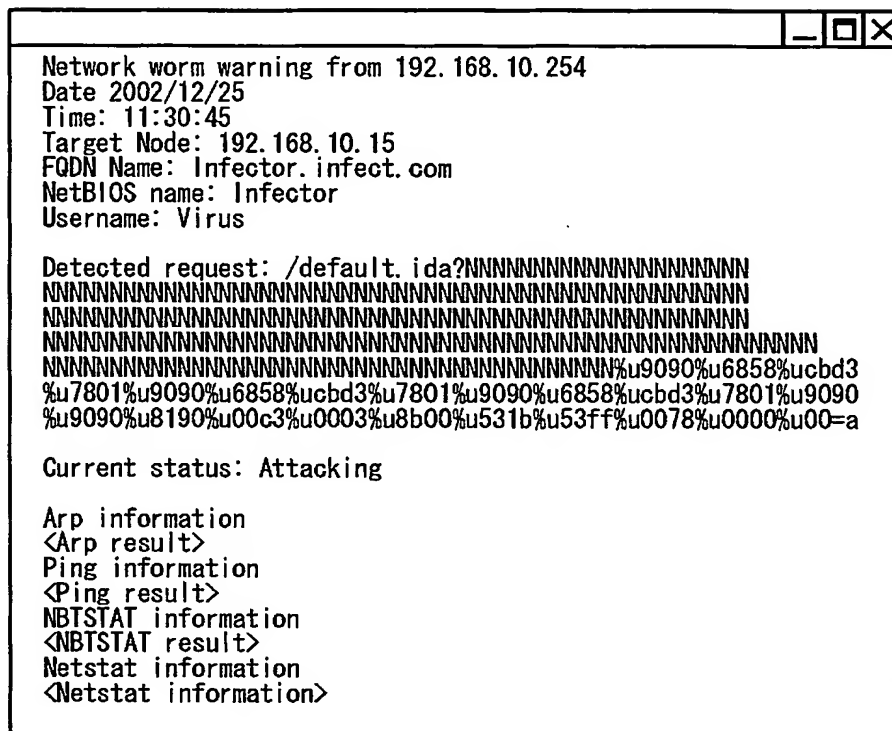
【符号の説明】

1 ネットワーク、 2 スピーカ、 3 ディスプレイ、 4 ネットワークインタフェース、 5 感染コンピュータ、 6 記憶装置、 7 ウィルス、 8 送信元 IP アドレス、 10 監視コンピュータ、 11 ネットワークインタフェース、 12 記憶装置、 13 おとりサーバ、 14 おとりフォルダ、 15 おとりアプリケーション、 16 通信情報解析手段、 17 コンピュータ攻撃手段、 18 検出報告送信手段、 19 警報発生手段

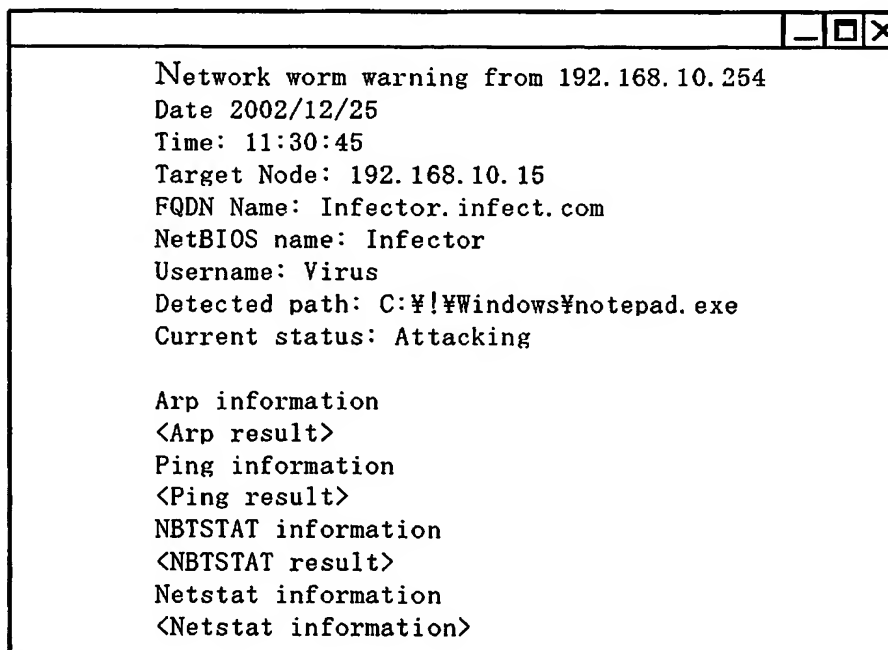




【図 2】

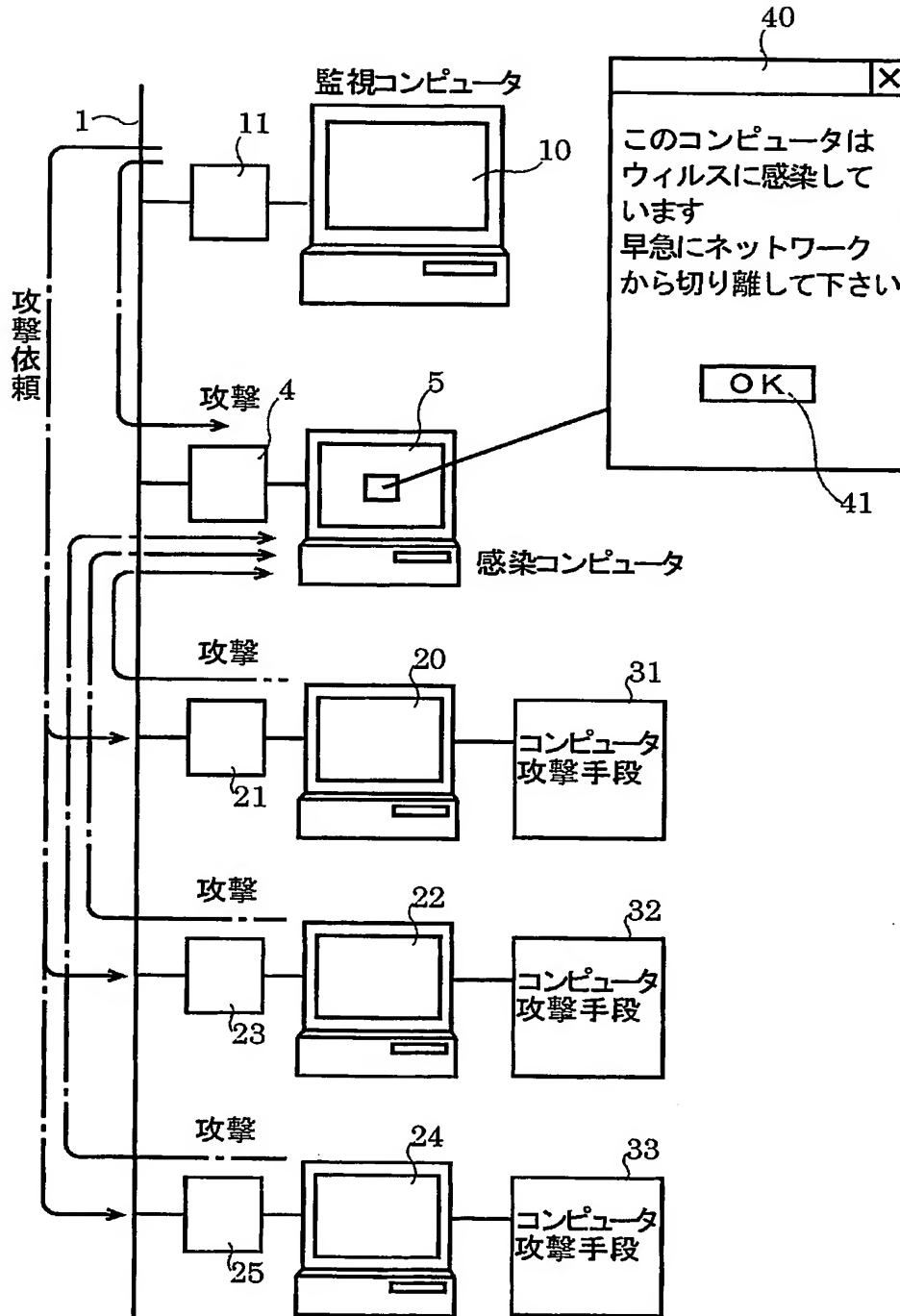


(a)

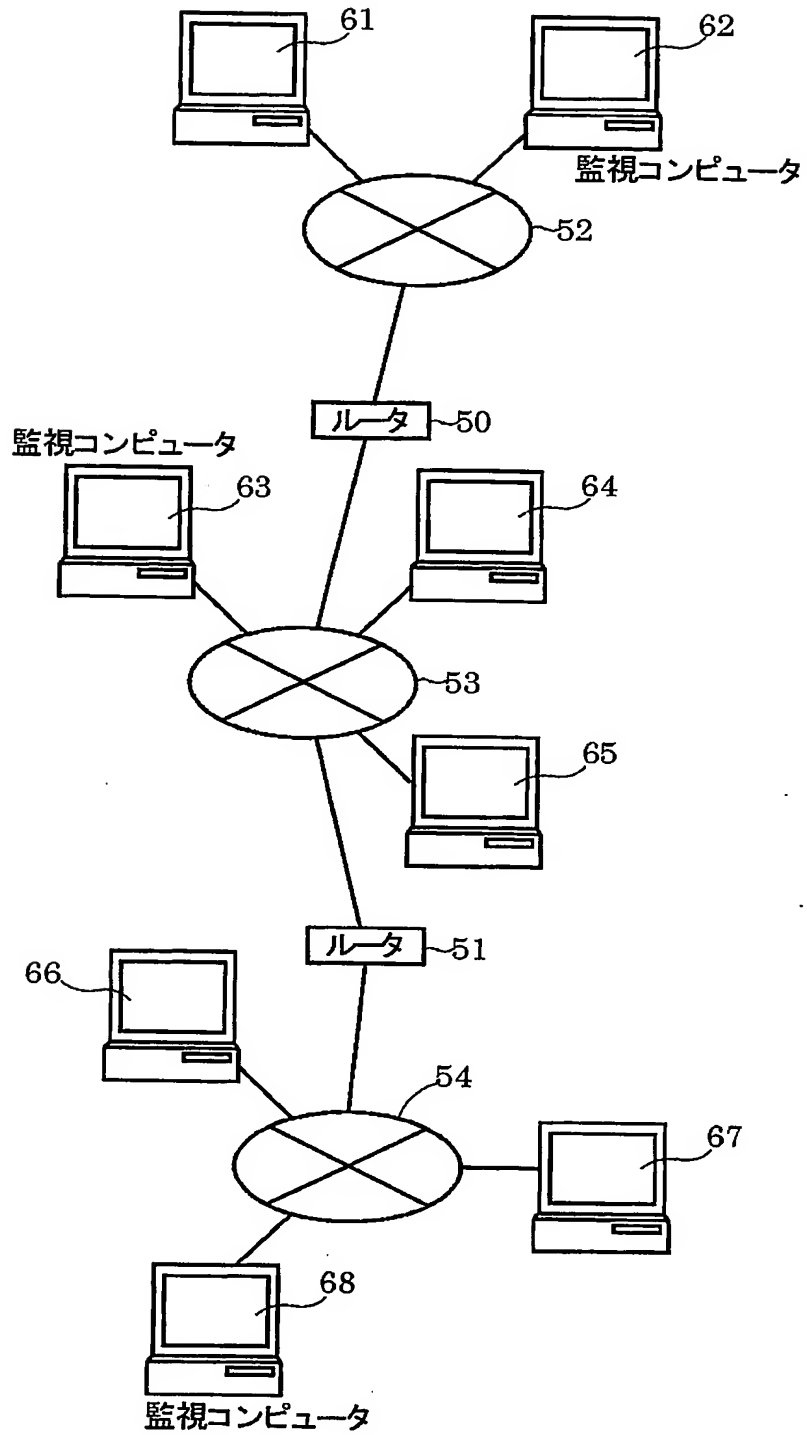


(b)

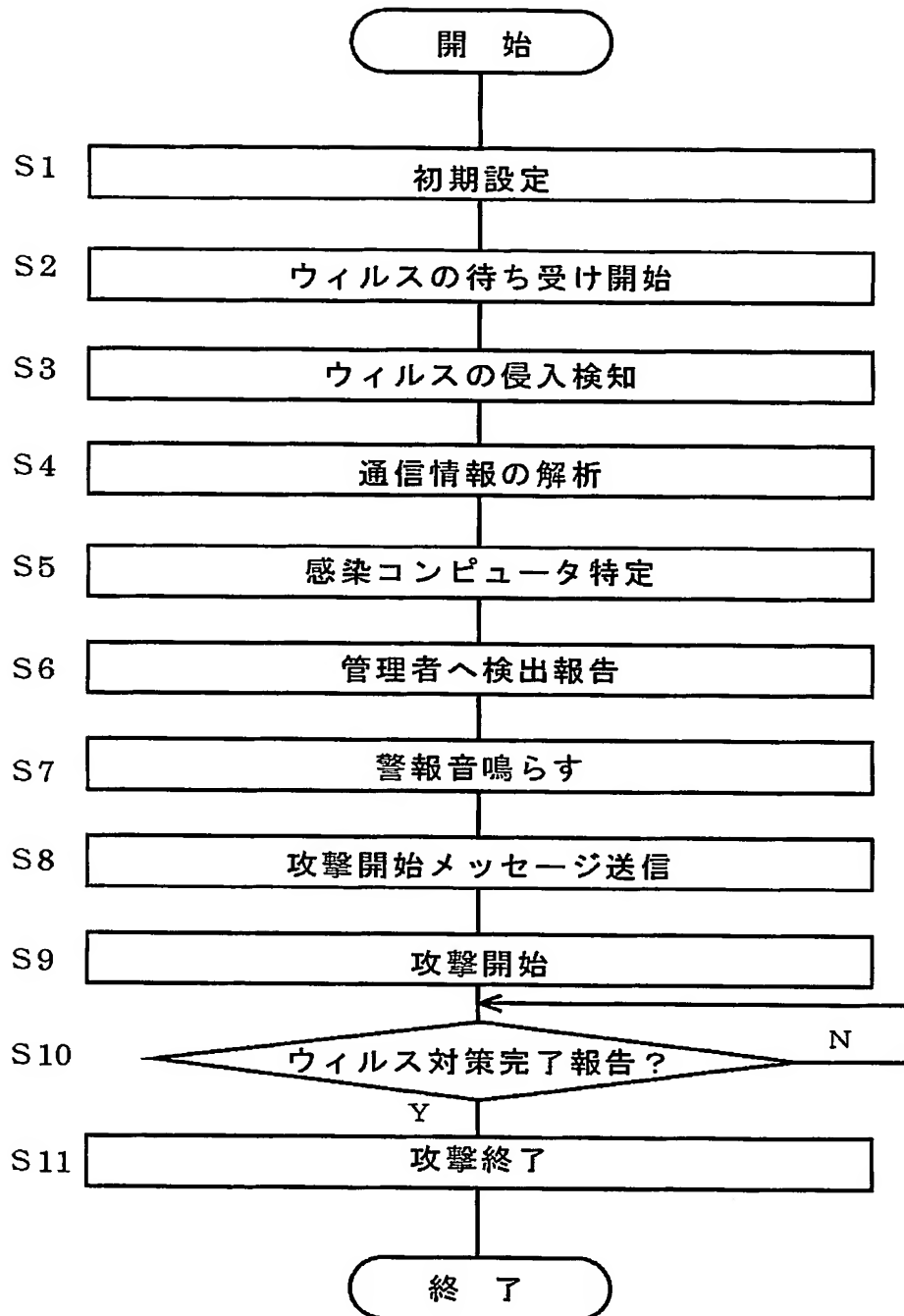
【図 3】



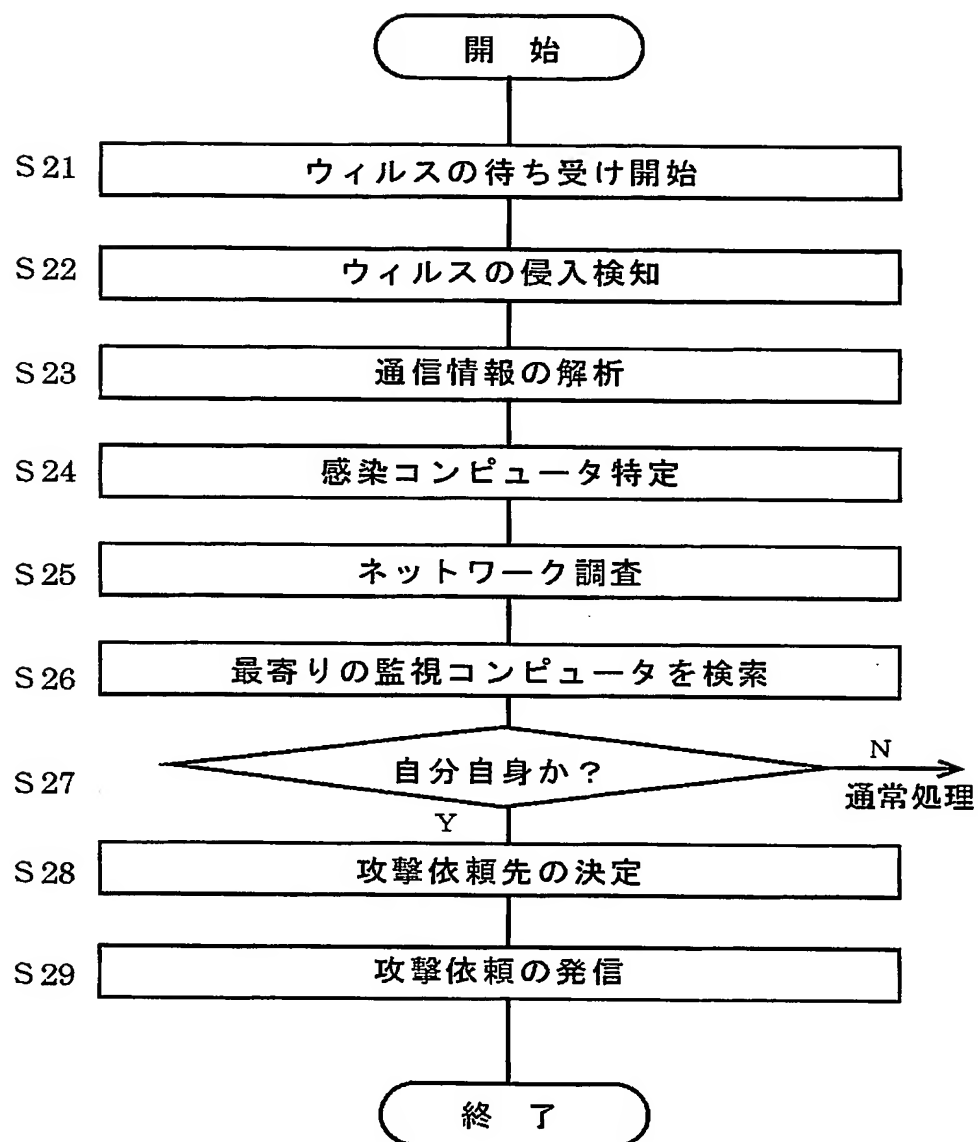
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 ネットワーク 1 を通じてサーバやフォルダに侵入するウィルスをいち早く検出して、被害の拡大を抑える。

【解決手段】 ウィルスに感染しているコンピュータ 5 を特定し、そのコンピュータ 5 の管理者がウィルスを除去する等の対策を終了するまでの間、監視コンピュータ 1 0 による攻撃を行う。そのコンピュータ 5 に高負荷を生じさせて、ウィルス 7 の活動を抑制する。ウィルス 7 に感染しているコンピュータ 5 を特定するためには、おとりのサーバ 1 3 等をネットワーク 1 中に構築する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2003-072371
受付番号	50300433936
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年 3月18日

<認定情報・付加情報>

【提出日】	平成15年 3月17日
-------	-------------

次頁無



特願 2 0 0 3 - 0 7 2 3.7 1

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 3 6 9 ]

1. 変更年月日

1 9 9 0 年 8 月 2 0 日

[変更理由]

新規登録

住 所

東京都新宿区西新宿 2 丁目 4 番 1 号

氏 名

セイコーエプソン株式会社